UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/534,541	05/10/2005	Yukio Tsuruoka	271813US90PCT	6985

22850 7590 08/29/2008
OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
SHEPELEV, KONSTANTIN	

ART UNIT	PAPER NUMBER
2131	

NOTIFICATION DATE	DELIVERY MODE
08/29/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

Office Action Summary	**Application No.** 10/534,541	**Applicant(s)** TSURUOKA ET AL.	
	Examiner KONSTANTIN SHEPELEV	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 May 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *5/10/2005, 10/12/2006*.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

This office action is in response to application filed on May 10, 2005 in which claims 1-23 are presented for examination.

Status of Claims

Claims 1-23 are pending; of which claims 1, 7, 12, and 15 are in independent form. Claims 21-23 are rejected under 35 USC 101. Claims 1-23 are rejected under 35 USC 103(a).

Specification

1. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

The following title is suggested: User authentication system for providing online services based on the transmission address.

Claim Rejections - 35 USC § 101

2. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 21-23 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 21 recites "program for allowing a computer to function" which is clearly a functional descriptive material, software, per se. When recorded on some computer-readable medium it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized. However, the claim language lacks the necessary computer readable medium, and as such fails to fall within one of four statutory categories of invention according to 35 U.S.C. 101. Therefore, claim 21 is non-statutory.

Claims 22 and 23 are rejected in view of the same reasons as stated in the rejection of claim 21.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 5-10, and 12-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Newcombe (US 2003/0172269 A1) in view of Arnold et al. (WO 03/055170 A1).

With respect to claim 1, Newcombe teaches the limitation of “an authentication system in which an authentication server which authenticates a user, a user terminal which transmits a user authentication information, and an application server which provides a service to the user through the user terminal are connected together to enable a communication therebetween through a network” (Fig. 1; page 2, paragraph

0025) as the system includes a client that desires access to a content server, application server, or the like. The authentication manager includes an application authentication server and ticket granting server.

Further, Newcombe teaches the limitation of “authentication means for authenticating a user based on the user authentication information transmitted as an authentication request from the user terminal” (page 3, paragraph 0044) as Application Authentication Server (AAS) is configured to authenticate a user.

Furthermore, Newcombe teaches the limitations of “a ticket issuing means for issuing a ticket containing the address allocated by the address allocating means” and “a ticket transmitting means for transmitting the ticket issued by the ticket issuing means to the user terminal” (page 4, paragraph 0044) as Application Authentication Server (AAS) is configured to provide the authenticated user one or more content tickets that enables authenticated user to access one or more content servers. The content ticket includes (page 4, paragraph 0048) the client’s local and remote IP addresses.

In addition, Newcombe teaches the limitation of “a user authentication information transmitting means for transmitting user authentication information to the authentication server for purpose of an authentication request” (page 4, paragraph 0052) as clients are enabled to request access to servers, such as content servers by requesting content tickets from AAS. Clients are enabled to provide information associated with local and remote IP addresses to AAS as part of the request for content tickets.

Additionally, Newcombe teaches the limitation of “a ticket reception means for receiving a ticket transmitted from the authentication server” (page 5, paragraph 0064) as Authentication Server (AS) determines the user is a valid user and provides client with a Ticket Granting Ticket. Where AS is a part of AAS (page 4, paragraph 0054).

Also, Newcombe teaches the limitations of “means for transmitting a packet including the ticket to the application server for establishing a session” and “a service request means for transmitting a packet requesting a service to the application server” (page 9, paragraph 0113) as client is to be authenticated by the content server. Where (page 10, paragraph 0114) authenticator and ticket is sent to the server.

Moreover, Newcombe teaches the limitation of “a ticket memory means for storing the ticket transmitted from the user terminal” (Fig. 4; page 4, paragraph 0056) as ADS is configured to provide storage for information associated with a client, user, ticket, and the like.

Furthermore, Newcombe teaches the limitation of “an address comparison means for determining whether or not the address contained in the ticket which is stored in the ticket memory means coincides with the source address of the service request packet which is transmitted from the user terminal through the session” (page 4, paragraph 0048) as Content server is also configured to read its portion of the content ticket to verify whether the sending client should be enabled access to the requested content. Where Newcombe teaches the process of validation (page 10, paragraph 0117) as a ticket, including an encrypted modified authenticator, is received. The client's local and remote IP addresses are obtained, and the encrypted modified authenticator is decrypted. Further, (page 10, paragraph 0119) a determination is made whether an remote IP address associated information provided be the client matches an IP address obtained by a variety of approaches, including a system call, examination of TCP/IP packets associated with the client, and the like.

Finally, Newcombe teaches the limitation of “a service providing means for transmitting to the user a packet which provides a service to the user when a coincidence between the addresses is determined by the address comparison means” (page 4, paragraph 0045) as Content server may include virtually any electronic device capable of storing content and sending the content to a requesting device.

It is noted, however, that Newcombe does not teach the limitations of “an address allocating means for allocating an address to the user terminal for a successful authentication of the user”, “means for setting up an address contained in the ticket as a source address for a packet which is to be transmitted from the user terminal.”

On the other hand, Arnold teaches the abovementioned limitation (page 5, lines 25-29) as an IP address is assigned to the user/subscriber during the single sign-on authentication procedure performed in the network of the respectively underlying network service provider of the user or the like.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Arnold into the system of Newcombe to allow the AAS to keep full control of the IP address assignment process in view of the limited pool of available IP addresses.

With respect to claim 5, Newcombe teaches the limitation of “the ticket issuing means of the authentication server comprises means including an authentication information generating means for generating an authentication information for a provisional ticket using a shared secret key which is shared beforehand between the authentication server and the application server and for issuing the ticket containing the authentication information” (page 6, paragraph 0068) as TGS is configured to receive the server readable portion of the TGT and modified authenticator from the user, and to provide a valid user with a content ticket that enables access to an identified content server. Furthermore, (page 6, paragraph 0071) the content ticket may include a server readable portion that is signed by a public encryption key associated with TGS.

In addition, Newcombe teaches the limitation of “the ticket verifying means of the application server comprising an authentication information verifier for verifying the presence or absence of any forgery in the authentication information contained in the ticket using a shared secret key which is beforehand shared between the authentication server and the application server and for preventing the ticket from being stored in the ticket memory means in the presence of a forgery” (Fig. 13; page 10, paragraphs 0126 - 0127) as a determination is made whether the client is authentic. If it is determined that the client is authentic, a determination is made whether information within the content ticket is valid. If the client is found not to be authentic or the information is not valid, an error message is sent to the client. Furthermore, (page 10, paragraph 0114) the authentication used for client authentication is encrypted using the session key obtained from the authentication server.

With respect to claim 6, Newcombe teaches the limitation of “a transmission of the ticket from the user terminal takes place in terms of a packet” (Abstract) as a packet that includes the authenticator is sent to a server.

In addition, Newcombe teaches the limitation of “the application server comprising an address collating means for collating the address in the ticket which is transmitted from the user terminal against the source address of the packet which includes the ticket and for preventing the ticket from being stored when a coincidence is not found” (Fig. 5; page 7, paragraph 0086 and 0087) as a client interacts with a Ticket Granting Server (TGS) to obtain a content ticket. If the client is unsuccessful, the processing ends. Where (page 10, paragraph 0119) a determination is made whether an remote IP address associated information provided be the client matches an IP address obtained by a variety of approaches, including a system call, examination of TCP/IP packets associated with the client, and the like.

With respect to independent claim 7, Newcombe teaches the limitation of “An authentication server in an authentication system in which an authentication of a user utilizing a user terminal is performed through the user terminal by an authentication server and a request is made to an application server to provide a service on the basis of the authentication” (Fig. 1; page 2, paragraph 0025) as the system includes a client that desires access to a content server, application server, or the like. The authentication manager includes an application authentication server and ticket granting server.

Further, Newcombe teaches the limitation of “a user authentication information reception means for receiving an authentication request inclusive of a user authentication information transmitted from the user terminal” (page 3, paragraph 0044) as Application Authentication Server (AAS) is configured to authenticate a user. Where, (page 4, paragraph 0052) clients are enabled to request access to servers, such as content servers by requesting content tickets from AAS. Clients are enabled to provide information associated with local and remote IP addresses to AAS as part of the request for content tickets.

Furthermore, Newcombe teaches the limitation of “an authentication means to which the user authentication information of the received authentication request is input and which authenticates the user on the basis of the user authentication information and providing a signal indicating a successful authentication upon a successful authentication” (page 5, paragraph 0064) as Authentication Server (AS) determines the user is a valid user and provides client with a Ticket Granting Ticket. Where AS is a part of AAS (page 4, paragraph 0054) and (page 10, paragraph 0115) a signal is provided that indicates whether the client is authentic or not.

In addition, Newcombe teaches the limitations of “a ticket issuing means to which the allocated address is input and which issues a ticket containing the address” and “and a ticket transmitting means to which the ticket is input and which transmits the ticket to the user terminal” (page 4, paragraph 0044) as Application Authentication

Server (AAS) is configured to provide the authenticated user one or more content tickets that enables authenticated user to access one or more content servers. The content ticket includes (page 4, paragraph 0048) the client's local and remote IP addresses.

It is noted, however, that Newcombe does not teach the limitation of "an address allocating means for allocating an address to the user terminal in response to an input of the signal indicating a successful authentication of the user."

On the other hand, Arnold teaches the abovementioned limitation (page 5, lines 25-29) as an IP address is assigned to the user/subscriber during the single sign-on authentication procedure performed in the network of the respectively underlying network service provider of the user or the like.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Arnold into the system of Newcombe to allow the AAS to keep full control of the IP address assignment process in view of the limited pool of available IP addresses.

With respect to claim 8, Newcombe teaches the limitation of "an authentication information generating means for generating an authentication information for information which includes at least the allocated address using a shared secret key which is beforehand shared between the authentication server and the application server" (page 4, paragraph 0044) as Application Authentication Server (AAS) is configured to provide the authenticated user one or more content tickets that enables authenticated user to access one or more content servers. The content ticket includes (page 4, paragraph 0048) the client’s local and remote IP addresses. Furthermore, (page 5, paragraph 0065) the client readable portion [of the ticket] is signed with the private key of the authentication server.

In addition, Newcombe teaches the limitation of “the ticket issuing means being means for issuing the ticket inclusive of the authentication information” (page 6, paragraph 0072) as if TGS determines that the client is valid and authorized, TGS is further configured to provide the client with the content ticket. Where, content ticket may include a server readable portion containing information associated with the client's local and remote IP addresses, the user's account, lifetime parameter, a portion of application content, such as an application title, version information or the like, and a session key.

With respect to claim 9, it is rejected in view of the same reasons as stated in the rejection of claim 8.

With respect to claim 10 as dependent upon claim 9, it is rejected in further view of the same reasons as stated in the rejection of claim 8.

With respect to claim 12, it is rejected in view of the same reasons as stated in the rejection of independent claim 1.

With respect to claim 13, Newcombe teaches the limitations of “a key information generating means to which a public key of the user terminal is input and which generates a key information relating to the public key” and “a session key generating means to which a private key of the user terminal and an public key of an application server are input and which calculates a session secret key which is shared with the application server” (paragraph 0029) as In one embodiment of the invention, for asymmetric encryption, 1024-bit keys may be used with RSA. These keys may be formatted according to the "OAEP (with SHA1)" scheme provided by RSA, or any other formatting appropriate. For example, RSA may be used in conjunction with a ticket (which is described in more detail below) to decrypt data in the ticket to recover an AES key that may then be used to decrypt other portions of a ticket. SHA1 stands for Secure Hash Algorithm 1. SHA1 is a cryptographic hash algorithm that produces a 160-bit hash value from an arbitrary length string. In other embodiments of the invention, other private key/public key encryption algorithms may be used (such as the ones listed above) with the same or different key sizes.

Further, Newcombe teaches the limitation of “a packet cryptographic processing means to which a packet to be transmitted from the user terminal and the session secret key are input and which applies a processing to the transmitted packet which guarantees that there is no forgery in the packet by the session secret key” (page 5, paragraph 0065) as client proves that it can decrypt the client readable portion be extracting the session key from client readable portion and using it to encrypt subsequent authenticators.

Finally, Newcombe teaches the limitation of “the user authentication information transmitting means being means to which the key information is also input and which transmits the key information together with the user authentication information” (page 4, paragraph 0052) as clients are enabled to provide information associated with local and remote IP addresses to AAS as part of the request for content tickets. Furthermore, (page 6, paragraph 0068) Ticket Granting Server (TGS) is configured to receive the server readable portion of TGT and modified authenticator from the user, where (page 6, paragraph 0072) the server readable portion may include information associated with the client’s local and remote IP addresses, the user’s account, lifetime parameter, a portion of application content, such as application title, version information or the like, and a session key.

With respect to claim 14, it is rejected in view of the same reasons as stated in the rejection of claim 13.

With respect to independent claim 15, it is rejected in view of the same reasons as stated in the rejection of independent claim 1.

With respect to claim 16, Newcombe teaches the limitation of “a ticket verifying means to which the ticket in the received packet is input and which verifies the authenticity of the ticket and prevents the ticket from being stored in response to a verification output which indicates the absence of the authenticity” (page 4, paragraph

0048) as Content server is also configured to read its portion of the content ticket to verify whether the sending client should be enabled access to the requested content. Where Newcombe teaches the process of validation (Fig. 13; page 10, paragraphs 0126 - 0127) as a determination is made whether the client is authentic. If it is determined that the client is authentic, a determination is made whether information within the content ticket is valid. If the client is found not to be authentic or the information is not valid, an error message is sent to the client. Furthermore, (page 10, paragraph 0114) the authentication used for client authentication is encrypted using the session key obtained from the authentication server.

With respect to claim 17, Newcombe teaches the limitation of “a session key generating means for calculating a session secret key which is shared with the user terminal from a private key of the application server and an public key of the user terminal” (paragraph 0029) as In one embodiment of the invention, for asymmetric encryption, 1024-bit keys may be used with RSA. These keys may be formatted according to the "OAEP (with SHA1)" scheme provided by RSA, or any other formatting appropriate. For example, RSA may be used in conjunction with a ticket (which is described in more detail below) to decrypt data in the ticket to recover an AES key that may then be used to decrypt other portions of a ticket. SHA1 stands for Secure Hash Algorithm 1. SHA1 is a cryptographic hash algorithm that produces a 160-bit hash value from an arbitrary length string. In other embodiments of the invention, other private key/public key encryption algorithms may be used (such as the ones listed above) with the same or different key sizes.

In addition, Newcombe teaches the limitation of “a packet verifying means for verifying whether or not a packet received from the user terminal is forged using the session secret key and for preventing the ticket from being stored in response to a verification output indicating the presence of a forgery” (page 5, paragraph 0065) as the server decrypts the server readable portion and extracts its copy of the session key, and uses that to decrypt the authenticator. If the authenticator is decrypted successfully then this proves beyond reasonable doubt that the client had the correct session key.

With respect to claim 18, it is rejected in view of the same reasons as stated in the rejection of claim 17.

With respect to claim 19, Newcombe teaches the limitation of “the ticket verifying means is means which an authentication purpose shared secret key which is shared with the user terminal and a session dependent information which changes each time a session is established are input and which processes the session dependent information using the authentication purpose shared secret key, collates a result of the processing against the key information in the ticket and verifies the authenticity of the ticket by seeing whether or not a matching between the result of processing and the key information applies” (page 4, paragraph 0048) as Content server is also configured to read its portion of the content ticket to verify whether the sending client should be enabled access to the requested content. Where the client is authenticated using the modified authenticator, and (page 2, paragraph 0025) the modified authenticator includes a timestamp that is combined with a cryptographically strong digest of a concatenation of the local and remote IP addresses associated with the client. The modified authenticator is directed at binding the timestamp to a single client to minimize theft and reuse of an authenticator.

With respect to claim 20, Newcombe teaches the limitation of "he ticket verifying means comprises means for verifying whether or not the source address of the received packet coincides with the address contained in the ticket within the packet and for preventing the ticket from being stored in response to a detection output which indicates a non-coincidence" (page 4, paragraph 0048) as Content server is also configured to read its portion of the content ticket to verify whether the sending client should be enabled access to the requested content. Where Newcombe teaches the process of validation (page 10, paragraph 0117) as a ticket, including an encrypted modified authenticator, is received. The client's local and remote IP addresses are obtained, and the encrypted modified authenticator is decrypted. Further, (page 10, paragraph 0119) a determination is made whether an remote IP address associated information provided be the client matches an IP address obtained by a variety of approaches, including a system call, examination of TCP/IP packets associated with the client, and the like. Furthermore, (Figs. 5 and 13; page 10, paragraph 0127) if the client is found not to be authentic or the information is not valid, an error message is sent to the client and the process returns to block 510 of Fig. 5, and consequently ends.

With respect to claim 21, it is rejected in view of the reasons stated in the rejection of independent claim 7.

With respect to claim 22, it is rejected in view of the same reasons as stated in the rejection of independent claim 12.

With respect to claim 23, it is rejected in view of the same reasons as stated in the rejection of independent claim 15.

4. Claims 2-4 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Newcombe (US 2003/0172269 A1) in view of Arnold et al. (WO 03/055170 A1) as applied to claim 1 above, and further in view of Medvinsky et al. (2003/0063750 A1).

With respect to claim 2, Newcombe teaches the limitation of “the ticket issuing means being means for issuing a ticket also containing the key information which is transmitted from the user terminal” (page 6, paragraph 0068) as Ticket Granting Server (TGS) is configured to receive the server readable portion of TGT and modified authenticator from the user, and to provide a valid user with a content ticket that enables access to an identified content server.

Further, Newcombe teaches the limitation of “the user authentication information transmitting means being means for transmitting the key information also together with the user authentication information” (page 4, paragraph 0052) as clients are enabled to provide information associated with local and remote IP addresses to AAS as part of the request for content tickets. Furthermore, (page 6, paragraph 0068) Ticket Granting Server (TGS) is configured to receive the server readable portion of TGT and modified authenticator from the user, where (page 6, paragraph 0072) the server readable portion may include information associated with the client’s local and remote IP addresses, the user’s account, lifetime parameter, a portion of application content, such as application title, version information or the like, and a session key.

Furthermore, Newcombe teaches the limitations of “a session key generating means for calculating a session secret key which is shared with the application server from a private key of the user terminal and a public key of the application server” and “a session key generating means for calculating a session secret key which is shared with the user terminal from the private key of the application server and a public key of the user terminal” (paragraph 0029) as In one embodiment of the invention, for asymmetric encryption, 1024-bit keys may be used with RSA. These keys may be formatted according to the "OAEP (with SHA1)" scheme provided by RSA, or any other formatting appropriate. For example, RSA may be used in conjunction with a ticket (which is described in more detail below) to decrypt data in the ticket to recover an AES key that may then be used to decrypt other portions of a ticket. SHA1 stands for Secure Hash Algorithm 1. SHA1 is a cryptographic hash algorithm that produces a 160-bit hash value from an arbitrary length string. In other embodiments of the invention, other private key/public key encryption algorithms may be used (such as the ones listed above) with the same or different key sizes.

In addition, Newcombe teaches the limitation of “a packet cryptographic processing means for performing a processing upon a packet transmitted from the user terminal to guarantee that there is no forgery in the packet by the session secret key” (page 5, paragraph 0065) as client proves that it can decrypt the client readable portion be extracting the session key from client readable portion and using it to encrypt subsequent authenticators.

Also, Newcombe teaches the limitations of “a packet verifying means for confirming whether or not the packet received from the user terminal is forged using the session secret key” and “a ticket verifying means for verifying whether or not the key information contained in the ticket of the packet which has been verified as not being forged is information relating to the private key of the user terminal” (page 5, paragraph 0065) as the server decrypts the server readable portion and extracts its copy of the session key, and uses that to decrypt the authenticator. If the authenticator is decrypted successfully then this proves beyond reasonable doubt that the client had the correct session key.

Finally, Newcombe teaches the limitation of “the ticket verifying means preventing the ticket from being stored in the ticket memory means when the key information is not a relating information” (Fig. 5; page 7, paragraph 0086 and 0087) as a client interacts with a Ticket Granting Server (TGS) to obtain a content ticket. If the client is unsuccessful, the processing ends.

It is noted, however, that Newcombe does not explicitly teach the limitation of "the user terminal has a key information relating to a private key of the user terminal."

On the other hand, Medvinsky teaches the abovementioned limitation as (page 2, paragraph 0019) a provisioning system that secures delivery of a client public key.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Medvinsky into the system of Newcombe to improve the security of the of the system

With respect to claim 3, Newcombe teaches the limitation of "a transmission of the ticket from the user terminal takes place in terms of a packet" (Abstract) as a packet that includes the authenticator is sent to a server.

In addition, Newcombe teaches the limitation of "an address collating means for collating the address in the ticket transmitted from the user terminal against the source address of the packet which includes the ticket and for preventing the ticket from being stored if a coincidence is not found" (Fig. 5; page 7, paragraph 0086 and 0087) as a client interacts with a Ticket Granting Server (TGS) to obtain a content ticket. If the client is unsuccessful, the processing ends. Where (page 10, paragraph 0119) a determination is made whether an remote IP address associated information provided be the client matches an IP address obtained by a variety of approaches, including a system call, examination of TCP/IP packets associated with the client, and the like.

With respect to claim 4, Newcombe teaches the limitation of “the authentication server comprises a user identifier allocating means for allocating a user identifier which corresponds to the authenticated user in response to the authentication request for a successful authentication of the user” (page 4, paragraph 0057) as Authentication Server (AS) is enabled to authenticate a user.

In addition, Newcombe teaches the limitation of “the ticket issuing means being means for issuing the ticket inclusive of the user identifier” (page 5, paragraph 0064) if AS determines that the user is a valid user, AS provides the client with a ticket granting ticket, that typically includes a server readable portion, client readable portion, and an authenticator.

With respect to claim 11, Newcombe teaches the limitation of “the ticket issuing means being means for issuing the ticket inclusive of the key information” (page 6, paragraph 0072) as if TGS determines that the client is valid and authorized, TGS is further configured to provide the client with the content ticket. Where, content ticket may include a server readable portion containing information associated with the client's local and remote IP addresses, the user's account, lifetime parameter, a portion of application content, such as an application title, version information or the like, and a session key.

It is noted, however, that Newcombe does not explicitly teach the limitation of “key information relating to a private key of the user terminal is contained in the authentication request.”

On the other hand, Medvinsky teaches the abovementioned limitation (page 2, paragraph 0023) as the method further comprises a ticket granting ticket obtained with the AS Request that is authenticated using a public key previously registered with the provisioning ticket.

It would have been obvious to one of the ordinary skill in the art to incorporate teachings of Medvinsky into the system of Newcombe because use it would provide a safer method for distributing authentication requests.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KONSTANTIN SHEPELEV whose telephone number is (571)270-5213. The examiner can normally be reached on Mon - Thu 8:30 - 18:00, Fri 8:30 - 17:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner’s supervisor, Ayaz R. Sheikh can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Konstantin Shepelev/ 8/26/2008
Examiner, Art Unit 2131
/Ayaz R. Sheikh/
Supervisory Patent Examiner, Art Unit 2131